Ochrona danych w placówce oświatowej.

Radosław Wiktorski. VULCAN.

W ostatnim czasie zagadnienie bezpieczeństwa informacji, a w szczególności ochrony danych osobowych nabrało dużego znaczenia. Wydaje się, iż główną przyczyną tego zjawiska jest zmieniający się świat, zwłaszcza w kontekście rozwoju technologii i jej powszechnego wykorzystania. Jeszcze kilka lat temu portale społecznościowe czy załatwianie spraw urzędowych przez Internet były nieznane, a o niektórych pojęciach (np. cloud computing – tzw. przetwarzanie danych w chmurze) nikt nie słyszał, zaś ochrona danych osobowych kojarzyła się jedynie z pustymi polami na listach lokatorów w blokach mieszkalnych. Dziś jest inaczej.

Szkoła, czy inna placówka oświatowa jest z punktu widzenia ochrony danych osobowych miejscem szczególnym. Bardzo dużo tu różnorodnych danych, w tym również danych zaliczanych do kategorii szczególnie chronionych (tzw. danych wrażliwych). Dane te przetwarza wiele osób, w bardzo różnorodny sposób. Szkoła również odczuwa rozwój technologii. Zaledwie kilka lat temu pierwsze systemy elektronicznej rekrutacji traktowane były jako novum, dziennik elektroniczny był bardziej ideą niż faktem, o możliwości otrzymywania na bieżąco informacji o ocenach bądź nieobecnościach dziecka w postaci wiadomości SMS na telefon komórkowy rodzica nawet nie wspominając. Dziś nie tylko są to już fakty, ale powoli staje się to standardem. To wszystko sprawia, że właściwa ochrona przetwarzanych danych staje się dla dyrektora prawdziwym wyzwaniem.

Z punktu widzenia osoby zarządzającej przedszkolem, szkołą bądź inną placówką oświatową (a tak naprawdę, to każdą organizacją, która w swoich działaniach przetwarza dane) na zagadnienie ochrony danych osobowych należy spojrzeć w dwóch aspektach: spełniania norm i obowiązków wynikających z obowiązującego prawa oraz realnie wdrażanych środków służących zapewnieniu bezpieczeństwa informacji, stosowanych również do chronienia innych danych niż osobowe. W niniejszych rozważaniach zostanie położony nacisk na pierwszy z tych aspektów.

Szereg wspomnianych wyżej zmian, związanych między innymi z rozwojem technologii, w połączeniu z jednej strony z jeszcze dość powszechną nieznajomością obowiązujących przepisów, z drugiej zaś z pewnym stopniem skomplikowania i nieintuicyjności tych regulacji sprawia, że w tematyce ochrony danych osobowych funkcjonuje szereg obiegowych opinii, często mijających się z rzeczywistością. Podstawowym celem wystąpienia jest z jednej strony obalenie funkcjonujących mitów, z drugiej zaś wskazanie zagadnień kluczowych, które powinny być przedmiotem zainteresowania i troski każdego dyrektora.

Administrator danych

Jednym z podstawowych, a jednocześnie niezmiernie ważnych pojęć, które pojawiają się w regulacjach dotyczących ochrony danych osobowych jest administrator danych (Art. 7 ust. 4 Ustawy o ochronie danych osobowych). W większości przypadków, z którymi mamy do czynienia w oświacie, niekiedy wbrew obiegowym opiniom, raczej nie można mieć wątpliwości, kto jest administratorem danych. W zakresie danych o uczniach, przedszkolakach, wychowankach, czy pracownikach **każdy dyrektor placówki powinien do siebie odnosić wszystkie obowiązki, uprawnienia i odpowiedzialność nakładane przepisami prawa na administratora danych**.

Biorąc pod uwagę obowiązujące przepisy, wśród obowiązków dyrektora należy wskazać przede wszystkim:

- **dołożenie szczególnej staranności** przy przetwarzaniu danych osobowych i ich zabezpieczaniu w celu ochrony interesów osób, których dane dotyczą. Powinno się to odbywać w szczególności poprzez zapewnienie w kierowanej przez siebie jednostce przetwarzania danych osobowych w sposób zgodny z obowiązującym prawem, w tym dla zgodnych z prawem celów oraz zachowania zasady adekwatności zakresu przetwarzanych danych do celu ich przetwarzania,
- **stworzenie, wdrożenie i prowadzenie dokumentacji** związanej z ochroną danych osobowych,

- **nadawanie i odbieranie upoważnień** do przetwarzania danych osobowych oraz bieżące prowadzenie ewidencji osób upoważnionych,
- **zgłaszanie** Generalnemu Inspektorowi Ochrony Danych Osobowych (GIODO) do rejestracji zbiorów danych, które objęte są takim obowiązkiem,
- udzielanie wskazanych w przepisach informacji osobom, których dane dotyczą (realizowanie tzw. obowiązku informacyjnego).

Należy ponadto pamiętać, iż również do administratora danych odnoszą się, zawarte w ustawie, przepisy karne.

Pojęcie danych osobowych

Wskazanie administratora danych w większości przypadków nie nastręcza trudności. Dużo bardziej niejednoznacznym, a przez to niejednokrotnie problematycznym jest pojęcie danych osobowych.

Po pierwsze należy jednoznacznie stwierdzić, iż **nawet wąskie w zakresie informacje typu imię i nazwisko czy samodzielnie występujący numer PESEL są danymi osobowymi** w rozumieniu przepisów o ochronie tych danych. Podejście takie znajduje potwierdzenie zarówno w stanowisku GIODO, jak i orzecznictwie. Do kategorii mitów zatem należy zaliczyć twierdzenia, iż przy tego typu danych potrzebne jest „coś jeszcze", by były one danymi osobowymi.

Pamiętajmy także, iż pojęcie danych osobowych dotyczy wszystkich informacji dotyczących zidentyfikowanej osoby fizycznej, a nie tylko tych, które pozwalają ją zidentyfikować. Zatem jeżeli osoba jest już zidentyfikowana (np. poprzez numer PESEL), to wszystkie inne informacje, które jej przynależą będą również podlegały ochronie.

Warto w tym miejscu zwrócić uwagę na kwestię adresów e-mail. W określonych przypadkach również występujący choćby samodzielnie adres e-mail może być daną osobową. Oczywiście adresu typu abcd@efgh.pl do takiej kategorii zaliczyć nie można, ale już adresy konstruowane wedle schematu imie.nazwisko@nazwa_firmy.pl pozwalają zidentyfikować osobę, a zatem stanowią daną osobową.

Po drugie zaś **danymi osobowymi są również zestawy informacji, które pozwalają zidentyfikować osobę pośrednio, za pomocą różnego rodzaju czynników**, w tym między innymi jej cech fizycznych, fizjologicznych, umysłowych, ekonomicznych, kulturowych lub społecznych. Oznacza to, że za dane osobowe mogą być uznane informacje, które na pierwszy rzut oka w ogóle z tą tematyką nie są kojarzone (przykładowo stwierdzenie „łysy w okularach od matematyki…" w przypadku konkretnej szkoły może umożliwiać zidentyfikowanie określonego nauczyciela.

Intuicyjnie dane kojarzą się z tym, co może być zapisane za pomocą słów lub cyfr. Warto jednak pamiętać, iż **daną osobową jest również wizerunek**. Oznacza to, że analizując dane osobowe przetwarzane w szkole należy także brać pod uwagę zdjęcia oraz nagrania wideo (w tym na przykład z monitoringu).

Podstawa przetwarzania

Aby przetwarzanie jakichkolwiek danych osobowych było legalne, przetwarzający musi umieć wskazać podstawę prawną tego przetwarzania (tak zwaną przesłankę legalizującą przetwarzanie danych). W praktyce sprowadza się to do wskazania jednego z pięciu punktów ustępu 1 artykułu 23 ustawy o ochronie danych osobowych (lub dla danych szczególnie chronionych odpowiedniego punktu z art. 27 ust. 2 ustawy).

Często popełnianym błędem w rozumieniu zasady funkcjonowania podstawy przetwarzania danych jest nieuwzględnianie zakresu danych. Trzeba bowiem zdawać sobie sprawę, iż **w kontekście podstawy przetwarzania należy rozpatrywać konkretny zakres danych**. Dane osobowe tej samej osoby mogą być przez administratora danych przetwarzane na różnych podstawach prawnych. Przykładowo od kandydata do pracy można wymagać danych wprost wskazanych w Kodeksie Pracy. Składane aplikacje zawierają często znacznie szerszy zakres danych, na których przetwarzanie kandydat wyraża zgodę. W tego typu sytuacji dane tej samej osoby, obejmujące dane identyfikacyjne, historię zatrudnienia bądź wykształcenie będziemy przetwarzać na podstawie art. 23 ust. 1 pkt. 2 (jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku

wynikającego z przepisu prawa), zaś inne dane typu zainteresowania, zdjęcie (wizerunek) na podstawie art. 23 ust. 1 pkt. 1 (zgoda osoby, której dane dotyczą).
Istnienie przesłanki legalizującej i umiejętność jej właściwego wskazania jest jednym z kluczowych elementów legalności przetwarzania danych.

Powierzenie przetwarzania

Popularyzacja rozwiązań związanych z dziennikiem elektronicznym sprawiła, że temat powierzenia przetwarzania danych stał się dosyć nośny. Warto jednak zauważyć, iż **z powierzeniem przetwarzania danych osobowych możemy mieć (i często mamy) do czynienia w placówce oświatowej nie tylko w kontekście dziennika elektronicznego**. W naturalny sposób temat ten powinien kojarzyć się z wszystkimi systemami internetowymi wykorzystywanymi w szkole, a zawierającymi dane osobowe, gdy dane przetwarzane są (a w szczególności przechowywane) na serwerach zewnętrznych, ale także wszelkie operacje związane z danymi osobowymi wykonywane przez podmioty trzecie (w tym na przykład zespoły ekonomiczno-administracyjne szkół).
Powierzenie przetwarzania, czyli, najprostszym językiem mówiąc, zlecenie przez administratora danych wykonywania określonych działań na określonych danych przez podmiot trzeci wzbudza wiele, często niepotrzebnych kontrowersji. Przede wszystkim trzeba stwierdzić, iż (oczywiście **po spełnieniu narzuconych prawem warunków) jest to działanie w pełni legalne**, mające swoją określoną specyfikę.
Z formalnego punktu widzenia najważniejszym czynnikiem, o którym należy pamiętać jest konieczność **zawarcia z podmiotem przetwarzającym dane pisemnej umowy powierzenia przetwarzania danych**. Jej istnienie jest warunkiem koniecznym dla legalności prowadzenia takich działań. Warto w tym miejscu podkreślić, iż brak takiej umowy nie jest tylko uchybieniem obowiązkowi jej zawierania, ale może być podstawą pociągnięcia do odpowiedzialności karnej z tytułu udostępnienia danych podmiotowi nieuprawnionemu do ich otrzymania.
W umowie, o której mowa powyżej, powinny zostać dokładnie wskazane: cel przetwarzania danych w ramach tej umowy oraz zakres danych, jaki podmiot przetwarzający może przetwarzać. Szereg kontrowersji pojawia się wokół określenia w umowach tego typu zakresu danych. Nie istnieje jeden wzorzec tego typu zapisów. Wydaje się, iż należy do tego podejść w taki sposób, by mając wątpliwości w odniesieniu do konkretnej informacji o osobie można było, bazując na zapisach umowy jednoznacznie określić, czy ta dana jest objęta powierzeniem przetwarzania, czy nie. **To niekoniecznie oznacza wskazywanie w umowie wszystkich pojedynczych danych** (przykładowo można odnieść się do dokumentu zewnętrznego, na przykład opisu struktury zbioru w systemie, przepisu prawa lub innego źródła szczegółowo definiującego zakres danych). Odniesienia do dokumentów zewnętrznych często są dużo wygodniejsze i prostsze w praktyce.
W kontekście dziennika elektronicznego często pojawiającą się wątpliwością jest pytanie, czy aby wprowadzić w szkole dziennik elektroniczny, którego oprogramowanie jest zainstalowane i funkcjonuje na serwerach dostawcy tego rozwiązania, konieczne jest uzyskiwanie zgody rodziców. Jednoznacznie należy stwierdzić, iż **nie ma takiego obowiązku.** To administrator danych decyduje o celach i **środkach** przetwarzania danych, zatem w jego wyłącznej kompetencji jest dobór sposobu przetwarzania danych.
Powierzenie przetwarzania danych w wielu przypadkach niesie ze sobą liczne korzyści i może być wręcz wskazane (przykładowo zazwyczaj w realiach szkolnych, chcąc wprowadzić dziennik elektroniczny, wyposażony w możliwość zapoznawania się rodziców z informacjami w nim zawartymi za pośrednictwem Internetu nie jesteśmy w stanie zapewnić takiego poziomu bezpieczeństwa i niezawodności rozwiązania, jak profesjonalny dostawca takiego oprogramowania na swoich serwerach). Jednakże należy pamiętać, iż czynność ta **niesie ze sobą również zagrożenia i ryzyko**. Trzeba bowiem mieć świadomość, iż za całość procesu przetwarzania danych osobowych, w tym również w tej części, która realizowana jest przez podmiot zewnętrzny, **odpowiedzialność ponosi administrator danych**.
Najprostszy i jednocześnie najważniejszy wniosek z tego płynący jest taki, że dane należy powierzać do przetwarzania podmiotom, w stosunku do których mamy przekonanie, że zapewnią

właściwy poziom ich bezpieczeństwa. Pamiętajmy, że bezpieczeństwo systemu informatycznego, to nie tylko infrastruktura (np. nowoczesne serwery umieszczone w profesjonalnym data center), ale także – a może nawet przede wszystkim – **ludzie i ich kompetencje oraz stosowane procedury**. Warto więc przed podpisaniem umowy upewnić się, że podmiot, któremu powierzamy nasze dane posiada **warunki i potencjał** do ich właściwego chronienia.

Dokumentacja

Zagadnienie dokumentacji związanej z przetwarzaniem danych osobowych w organizacji, w tym w szczególności w placówce oświatowej, jest dość rozległe. Również w tym temacie funkcjonuje wiele obiegowych opinii, pojawia się szereg pytań i rozmaitych pomysłów.

Pierwszym faktem, co do którego nie ma chyba wątpliwości, jest **konieczność posiadania takich dokumentów**. Przyjrzyjmy się zatem na wstępie, z czego składa się dokumentacja, którą jako dyrektorzy placówek oświatowych, odpowiedzialni i realizujący wynikające z przepisów prawa zadania administratorów danych, powinniśmy mieć. Ustawa i jej przepisy wykonawcze nakazują nam **stworzyć, wdrożyć i prowadzić**:

- Politykę bezpieczeństwa,
- Instrukcję zarządzania systemami informatycznymi,
- Ewidencję osób upoważnionych do przetwarzania danych osobowych.

Polityka bezpieczeństwa jest dokumentem opisującym zasady postępowania z danymi, w szczególności osobowymi oraz zastosowane środki (zarówno techniczne, jak i organizacyjne) służące ich zabezpieczaniu. Przepisy prawa formułują kilka wymogów w zakresie zawartości tego dokumentu, przy czym są to elementy **konieczne, a nie wystarczające**. Nie istnieje formalny wzór takiego dokumentu ani szczegółowe wytyczne. W poszukiwaniach można odnieść się jedynie do Polskich Norm, jednak tam również nie znajdziemy kompletnych odpowiedzi. Podobnie rzecz się ma z Instrukcją zarządzania systemami informatycznymi, która jest dokumentem opisującym zasady funkcjonowania systemów informatycznych, przetwarzających dane osobowe.

Można zastanawiać się, czy brak tego typu wzorców jest przypadkowy czy zamierzony. Mocno uzasadnioną tezą wydaje się być stwierdzenie, że brak w przepisach prawa wzorców jest zamierzony. Należy bowiem zauważyć, iż **istotą tej dokumentacji jest opisanie stanu faktycznego, realiów konkretnej placówki** (organizacji), **stosowanych tam w rzeczywistości środków zabezpieczających dane, osadzonych na opisanych prawdziwie przebiegających procesach przetwarzania danych**. Takie podejście potwierdza się również w praktyce – jednym z podstawowych elementów każdej kontroli GIODO jest badanie zgodności stanu opisanego w dokumentacji ze stanem rzeczywistym.

Dokumentacja, o której mowa obejmuje swoim zasięgiem **całość procesów** dotyczących przetwarzania danych w placówce, zarówno realizowanych w systemach elektronicznych, jak i przetwarzania tradycyjnego (papierowego). Opisane w niej powinny zostać **wszystkie zbiory, wszystkie systemy i wszystkie zabezpieczenia**. Oznacza to, że zazwyczaj nie tworzy się odrębnych dokumentacji dla pojedynczych systemów czy pojedynczych procesów (np. dokumentacja związana z dziennikiem elektronicznym czy związana z obsługą matur) – wszystko opisuje się w jednym dokumencie, obejmującym swym zasięgiem całość organizacji.

Ważny i kluczowy wniosek z powyższych rozważań, obalający jednocześnie jeden z funkcjonujących mitów – „można wziąć gotowca", jest taki, że pojawiające się czasem w obiegu **szablony takiej dokumentacji, z punktu widzenia odpowiedzialnego dyrektora są bezużyteczne**. Specyfika działalności poszczególnych placówek, przejawiająca się bardzo różnie – na przykład organizacyjnie, technologicznie, lokalowo – **wymusza konieczność indywidualnego podejścia** do tworzonych dokumentów.

Ważnym elementem dokumentacji jest kwestia **upoważnień do przetwarzania danych osobowych oraz ewidencja osób upoważnionych**. Jeśli chodzi o same upoważnienia, to należy koniecznie pamiętać, iż ustawa pozwala administratorowi danych dopuszczać do przetwarzania jedynie osoby z nadanym upoważnieniem. **Ten błahy, mogło by się zdawać, obowiązek może**

rodzić poważne konsekwencje – przetwarzanie danych przez pracownika, któremu nie nadano uprzednio upoważnienia do przetwarzania danych można traktować jako udostępnienie danych osobie nieupoważnionej, za co administratorowi danych grożą sankcje karne przewidziane w ustawie.

Rozważając temat dokumentacji warto pamiętać o jej aktualizacji. **Dyrektor jest odpowiedzialny za to, by dokumentacja była aktualna i zgodna ze stanem faktycznym**. O ile Polityka bezpieczeństwa i Instrukcja zarządzania systemami informatycznymi są dokumentami stosunkowo stabilnymi (modyfikacje w nich dokonywane są w przypadku zmian w funkcjonowaniu placówki, na przykład wdrożenie nowego systemu, zmiany lokalowe, zmiany w strukturze organizacyjnej itp.), to ewidencja osób upoważnionych w praktyce zmienia się często. Fakt ten, w połączeniu ze wspomnianymi wcześniej konsekwencjami nienadawania upoważnień do przetwarzania danych sprawiają, iż **zagadnienie nadawania, odbierania i ewidencjonowania upoważnień do przetwarzania danych osobowych powinno stać się elementem standardowych procedur** obsługi kadrowej w jednostce, a także obsługi innych osób mających do czynienia z przetwarzaniem danych w placówce (kontrole, firmy współpracujące itp.)

Rejestracja zbiorów

Kolejnym zagadnieniem, które doczekało się dużej liczby mitów i obiegowych opinii jest obowiązek zgłoszenia zbiorów danych do rejestracji Generalnemu Inspektorowi Danych Osobowych. Przyjrzyjmy się zatem bliżej tej tematyce.

Ustawa o ochronie danych osobowych w artykule 40 **nakazuje administratorowi danych zgłaszać** zbiory danych osobowych do rejestracji Generalnemu Inspektorowi. Jednocześnie w artykule 43 ust. 1 **wskazane są wyjątki** od przedstawionej powyżej reguły. Przed analizą wspomnianych wyjątków warto zwrócić uwagę na kwestię pojęcia zbioru. Po pierwsze zgłoszeniu do rejestracji podlegają zbiory danych osobowych w rozumieniu definicji zawartej w ustawie (art. 7 pkt. 1). Po drugie zaś o tym, z jakimi zbiorami mamy do czynienia decyduje administrator danych, czyli w praktyce dyrektor placówki. **Identyfikacja zbiorów danych ma miejsce w dokumencie Polityki bezpieczeństwa.** Pamiętajmy zatem, że rozpatrywanie ewentualnego obowiązku zgłoszenia zbioru danych do rejestracji będzie zawsze dokonywane w kontekście zdefiniowanych uprzednio zbiorów. Jest to kolejny powód, dla którego **ważne jest po pierwsze indywidualne, a po drugie przemyślane podejście** do tworzenia, opisywanej wcześniej, dokumentacji.

Ustawodawca przewidział szereg przypadków, w których administrator danych jest zwolniony z obowiązku zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi. Pełny ich katalog znajduje się w artykule 43 ust. 1 ustawy. W tym miejscu warto zwrócić uwagę na trzy spośród nich. W myśl tych zapisów z obowiązku zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi zwolnieniu są administratorzy danych:

- przetwarzanych w związku z zatrudnieniem u nich, świadczeniem im usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się,
- przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej,
- powszechnie dostępnych.

Patrząc na powyższe należy stwierdzić, iż z punktu widzenia dyrektora placówki oświatowej **nie ma obowiązku zgłaszania do rejestracji** zbiorów danych obejmujących uczniów, pracowników oraz danych księgowych. W kontekście **zgłoszenia do rejestracji należy rozpatrywać** w szczególności takie kategorie danych, jak kandydaci do przedszkola/szkoły oraz dzieci obwodowe.

Realizacja samego procesu zgłoszenia jest stosunkowo prosta i zazwyczaj nie nastręcza trudności. Wzór wniosku zgłoszenia określony jest w rozporządzeniu, zaś system elektroniczny na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych (http://giodo.gov.pl) ułatwia jego wypełnienie. Trzeba jednak pamiętać, iż **informacje zawarte we wniosku powinny być zgodne z rzeczywistością**, a zgodność ta w przypadku ewentualnej kontroli ze strony inspektorów GIODO będzie z pewnością weryfikowana. Z drugiej strony warto też zwrócić uwagę, **czy opisany**

we wniosku stan faktyczny jest zgodny z prawem (np. fakt posiadania stosownej dokumentacji, upoważnienia właściwych osób, powierzenia przetwarzania).

Odpowiedzialność

Na zakończenie warto krótko przyjrzeć się kwestii odpowiedzialności za przestrzeganie przepisów dotyczących ochrony danych. Zagadnienie to jest oczywiście wieloaspektowe. W tym miejscu zostanie zwrócona uwaga na aspekt jednoznaczności tej odpowiedzialności.

Na rynku, również na rynku edukacyjnym, można spotkać w różnych sytuacjach powoływanie się przez producentów bądź dostawców na zewnętrzne opinie, certyfikaty bądź innego rodzaju analizy potwierdzające określone okoliczności lub stwierdzające określone fakty (np. legalność przetwarzania). Jednoznacznie trzeba stwierdzić, iż **tego typu dokumenty w praktyce mają charakter wyłącznie marketingowy**.

Administrator danych, w imieniu którego działa dyrektor jednostki, ponosi odpowiedzialność za wszystkie procesy przetwarzania danych osobowych w podległej mu organizacji. W szczególności dotyczy to na przykład doboru wykorzystywanego oprogramowania. Fakt, iż jakikolwiek inny podmiot (w praktyce komercyjny) stwierdził, że dane oprogramowanie spełnia wymogi przepisów o ochronie danych osobowych w żaden sposób **nie wyłącza, ani nawet nie ogranicza odpowiedzialności dyrektora** za zgodność stosowanych środków przetwarzania danych z wymogami prawa.

Powyższe znalazło również potwierdzenie w oficjalnym wystąpieniu Generalnego Inspektora Ochrony Danych Osobowych, który stwierdził: *Generalny Inspektor Ochrony Danych Osobowych, ani żaden inny podmiot, nie wydaje certyfikatów, których posiadanie jest warunkiem legalności przetwarzania danych. Zatem ewentualne certyfikaty wydane przez inne podmioty nie mają znaczenia z punktu widzenia dopuszczalności przetwarzania danych przez posiadacza takiego dokumentu*.

Odpowiedzialność dyrektora jednostki za procesy przetwarzania danych osobowych w podległej mu placówce jest **jednoznaczna i rozległa**. Dobrze jest zatem zwrócić szczególną uwagę na to zagadnienie, podjąć działania stanowiące i porządkujące, by unormować ten aspekt funkcjonowania placówki. W tych działaniach warto korzystać z kompetencji zewnętrznych – ułatwia to i przyspiesza szereg działań. Długoterminowo zaś zagadnienia ochrony danych osobowych, a w szczególności bieżący nadzór nad tymi procesami, powinny dołączyć do rutynowych czynności zarządczych każdego dyrektora.